

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

---

United States of America,

v.

Caswell Senior, *et al.*,

Defendants.

---

:  
:  
:  
:  
:  
:  
:  
:  
:

No. 20 Cr. 626 (PMH)

**MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT  
CASWELL SENIOR'S PRETRIAL MOTIONS**

James Kousouros, Esq.  
Stuart Gold, Esq.  
The Law Offices of James Kousouros  
260 Madison Avenue, 22nd Floor  
New York, NY 10016  
P: (212) 532-1934  
F: (212) 532-1939  
james@kousouroslaw.com  
stuart@kousouroslaw.com  
*Counsel for Defendant Caswell Senior*

**TABLE OF CONTENTS**

PRELIMINARY STATEMENT ..... 1

FACTUAL STATEMENT ..... 1

    I.    Text Messages and Potential Preservation/Authentication Issue ..... 1

    II.   Search Warrant for Mr. Senior’s Apple iCloud Records..... 3

    III.  The Operative Indictment..... 7

ARGUMENT..... 7

    I.    THE iCloud WARRANT VIOLATED THE FOURTH AMENDMENT ..... 8

        A.    The Agent’s Affidavit Did Not Provide Probable Cause to Believe that Evidence of the  
Subject Offenses Would be Found on Mr. Senior’s iCloud Account ..... 9

        B.    The iCloud Warrant was Fatally Overbroad..... 13

        C.    The iCloud Warrant Was Insufficiently Particular..... 16

        D.    Other Unconstitutional Infirmities of the iCloud Warrant ..... 20

            Lack of Temporal Limitations ..... 20

            Authorization to Search All Devices ..... 21

            Evidence Unrelated to the Subject Offenses ..... 21

    II.   THE GOVERNMENT SHOULD BE REQUIRED TO PROVIDE 404(B) EVIDENCE  
SIXTY DAYS BEFORE TRIAL ..... 22

    III.  THE GOVERNMENT SHOULD DISCLOSE ALL EXCULPATORY AND  
IMPEACHMENT MATERIAL FORTHWITH..... 22

RESERVATION CLAUSE..... 24

CONCLUSION ..... 24

## **TABLE OF AUTHORITIES**

### **Cases**

<i>Brady v. Maryland</i> , 373 U.S. 83 (1963) .....	22
<i>Giglio v. United States</i> , 405 U.S. 150 (1972) .....	23
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004) .....	17
<i>In re 650 Fifth Ave. &amp; Related Properties</i> , 830 F.3d 66 (2d Cir. 2016) .....	13
<i>Kyles v. Whitley</i> , 514 U.S. 419 (1995) .....	23
<i>Riley v. California</i> , 573 U.S. 373 (2014) .....	8
<i>U.S. Postal Serv. v. C.E.C. Servs.</i> , 869 F.2d 184 (2d Cir. 1989) .....	14
<i>United States v. Agurs</i> , 427 U.S. 97 (1976) .....	23
<i>United States v. Bagley</i> , 473 U.S. 667 (1985) .....	22
<i>United States v. Cardwell</i> , 680 F.2d 75 (9th Cir. 1982) .....	18
<i>United States v. Drago</i> , No. 18-cr-394, 2019 WL 4364644 (E.D.N.Y. June 25, 2019) .....	14
<i>United States v. Ganas</i> , 755 F.3d 125 (2d Cir. 2014) .....	8
<i>United States v. George</i> , 975 F.2d 72 (2d Cir. 1992) .....	18
<i>United States v. Gigante</i> , 979 F. Supp. 959 (S.D.N.Y. 1997) .....	18
<i>United States v. Griffith</i> , 867 F.3d 1265 (D.C. Cir. 2017) .....	21
<i>United States v. Lnu</i> , 575 F.3d 298 (3d Cir. 2009) .....	3
<i>United States v. Nieto</i> , 76 M.J. 101 (C.A.A.F. 2017) .....	10
<i>United States v. Perez</i> , 116 F.3d 840 (9th Cir. 1997) .....	18
<i>United States v. Purcell</i> , 967 F.3d 159 (2d Cir. 2020) .....	6, 8, 13
<i>United States v. Raymonda</i> , 780 F.3d 105 (2d Cir. 2015) .....	9
<i>United States v. Rizzo</i> , 491 F.2d 215 (2d Cir. 1974) .....	3
<i>United States v. Roche</i> , 614 F.2d 6 (1st Cir. 1980) .....	19
<i>United States v. Shipp</i> , 392 F. Supp. 3d 300 (E.D.N.Y. 2019) .....	21
<i>United States v. Vilar</i> , No. 05-cr-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007) .....	15, 18
<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017) .....	13, 14
<i>United States v. Whitten</i> , 706 F.2d 1000 (9th Cir. 1983) .....	18
<i>United States v. Wong</i> , 78 F.3d 73 (2d Cir. 1996) .....	23
<i>Utah v. Strieff</i> , 579 U.S. 232 (2016) .....	8

**Statutes**

18 U.S.C. § 924(c) .....4

18 U.S.C. § 1962(d).....4

18 U.S.C. § 2518(8)(a) .....3

**Federal Rules**

Fed. R. Crim. P. 16 .....1, 22

Fed. R. Evid. 404(b) .....1

Fed. R. Evid. 901(a).....3

### **PRELIMINARY STATEMENT**

Defendant Caswell Senior submits this memorandum of law in support of his pretrial motions for an Order: (i) granting the defense leave to file additional motions depending on the outcome of outstanding discovery issues related to the preservation and authentication of text messages provided to the defense pursuant to Fed. R. Crim. P. 16; (ii) suppressing evidence seized pursuant to a warrant to search Mr. Senior's Apple iCloud account; (iii) directing that the Government reveal any evidence it intends to introduce at trial pursuant to Fed. R. Evid. 404(b) sixty days before trial; (iv) directing the pretrial disclosure of all exculpatory and impeachment material; (v) permitting Defendants to file additional motions which may arise from the requests made herein; and (vi) to provide any such further relief as the Court may deem proper and in the interest of justice.

Counsel for Defendants Christopher Erskine, Dwight Reid, Isaiah Santos, Brandon Soto, Deshawn Thomas, Ahmed Walker and Robert Wood join in these motions where applicable.

### **FACTUAL STATEMENT**

In or about March 2020, the FBI began a criminal investigation of an alleged Bloods gang known as the Untouchable Gorilla Stone Nation ("Gorilla Stone"). In the course of the investigation, the Government obtained, *inter alia*, wiretap warrants for the cellphones of Codefendants Austin, Erskine, Luster, and Walter and obtained a search warrant for Mr. Senior's iCloud account. Subsequently, Defendants were indicted for various crimes, including racketeering, drug trafficking, and firearm crimes.

#### **I. Text Messages and Potential Preservation/Authentication Issue**

Pursuant to the court-ordered Title III wiretaps, the FBI intercepted and recorded text messages (among other communications) over cellphones belonging to several defendants. A

district judge physically sealed the container holding the original recordings of the intercepted communications.

During the initial stages of providing Rule 16 discovery, the Government provided the court-appointed discovery coordinator, Julie de Almeida, Esq., with a drive containing audio files and text messages that were generated by a machine called “Green Tiger.” Ms. de Almeida reviewed the drive and noticed that while we were provided with “linesheets” for text messages, the underlying data, to wit, the “native files,” were not contained on the drive. Ms. de Almeida informed the Government and the defense of this finding.

What followed was months of discussion, pursuant to Local Criminal Rule 16.1, during which the Government followed up with the monitoring agents to ascertain whether the data had been provided and, if not, whether it had been preserved. The undersigned discussed the issue with the Government in February 2022 as we still did not have the native files and were therefore contemplating a motion to preclude evidence of the text messages. Ms. de Almeida continued her dialogue with the Government as well.

In March 2022, the Government provided Ms. de Almeida with its original FBI drive, suspecting that the missing files had not been properly copied. After further investigation, it was learned that the first drive produced by the Government contained copy errors (i.e., there were files missing from the first drive we received that were on the second); however, these files did not resolve the native files issue. The second “original” drive, containing over six million files, did not contain all of the native files for the text messages.

On March 14, 2022, the Government informed Ms. de Almeida that the drive that the FBI provided to the Government was the working copy (DCS6000) requiring FBI proprietary programs to access, rather than DCS5000 which is the discovery copy. The discovery copy would be decrypted and would include the audio files (.wav), sri files, xml, and html index files with the text

messages. The DCS5000 drive will be made available to Ms. de Almeida during the week of March 21, 2022. Upon her review of the drive, she will be able to discern whether the native files have been produced and can be meaningfully reviewed.

Defendants respectfully reserve the right to move to exclude evidence of the intercepted texts until after counsels' receipt and review of the new discovery drive. *See* 18 U.S.C. §§ 2518(8)(a), 2517(3); *United States v. Lnu*, 575 F.3d 298, 303–04 (3d Cir. 2009) (“Section 2518(8)(a)’s clear focus is on preserving the accuracy and authenticity of the contents of the wiretap recordings used and disclosed at trial.”); Fed. R. Evid. 901(a) (“To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”); *United States v. Rizzo*, 491 F.2d 215, 217 & n.7 (2d Cir. 1974) (providing that the Government bears the initial burden of making a prima facie showing of reasonable minimization in connection with intercepted communications).<sup>1</sup>

## **II. Search Warrant for Mr. Senior’s Apple iCloud Records**

On August 24, 2020, an FBI agent (the “Agent”) submitted to a magistrate judge (the “Magistrate”) an affidavit in support of an application for a search warrant for “all content and other information associated” with Mr. Senior’s Apple iCloud account (referred to as “Subject Account-3” in the affidavit). (Ex. A, iCloud Warrant Aff., ¶ 1). The Agent submitted this affidavit based on his “personal knowledge,” review of “documents and other evidence,” “conversations with other law enforcement officers,” and “training and experience concerning the use of email in criminal activity.” (*Id.* ¶ 3).

---

<sup>1</sup> When quoting cases and other materials, all internal quotation marks, citations, brackets, and footnotes are omitted unless otherwise indicated.

In his affidavit, the Agent alleged the following about the iCloud service: (1) iCloud is a “file hosting, storage, and sharing service” that “can be utilized through numerous iCloud-connected services,” which “allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connect device”; (2) “Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space”; (3) the storage space “may contain data associated with the use of iCloud-connected services”; and (4) iCloud “can also be used to store iOS device backups and data associated with third-party apps” (e.g., WhatsApp “can be configured to regularly back up a user’s instant messages on iCloud drive”). (*Id.* ¶¶ 4, 6(c), 12).

The Agent then swore that there was probable cause to believe that Mr. Senior’s iCloud account contained “evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1962(d) and 1959 et seq. (RICO conspiracy and violent crime in aid of racketeering); 924(c) (possession and use of a firearm in furtherance of a narcotics trafficking crime and/or a crime of violence); 922(g)(1) (felon in possession of a firearm or ammunition) and 21 U.S.C. § 846 (conspiracy to distribute narcotics) (‘the Subject Offenses’).” (*Id.* ¶ 3). In support, the Agent alleged the following:

- In August 2019, Codefendant Deshawn Thomas posted on Instagram a photograph that “shows [him], Senior, and many other Gorilla Stone members ... making the Gorilla Stone hand symbol.” In October 2019, Codefendant Walter Luster posted on Instagram a photo that “shows Luster making the Gorilla Stone hand symbol (the shape of a diamond) with Caswell Senior.” “During [three-way] prison calls on the Senior Cellphone [a cellphone belonging to Mr. Senior with a number ending in 0443] in June and July 2020, Luster, Senior, and Reid have discussed, among other things, Senior [a rapper] making cash payments to Reid for Reid’s role in Senior’s music career, and Senior’s promotion of Gorilla Stone.” “Based on my review of the contents of [Codefendant Donovan Gillard’s] iCloud [a]ccount, I know that Gillard ... had pictures with Senior and other Gorilla Stone members making gang signs on the Gillard iCloud Account, and it appears that some of

the pictures were initially posted to an Instagram Account used by Senior.”<sup>2</sup> (*Id.* ¶¶ 28–31).

- On July 7, 2020, Luster posted on Instagram a photo that “shows Luster [by himself] holding a firearm.” “Based on my review of two prison calls made by Reid to Luster on July 7, 2020, I know that Luster, Thomas, and Senior were together on July 7, 2020—the date the above picture of Luster holding a firearm was posted to the Luster Instagram Account—and were coming back from a trip to Miami.” Because Mr. Senior has “a prior felony conviction” it “would ... be illegal for [him] to have possessed the firearm seen in the above picture on July 7, 2020.” (*Id.* ¶ 28 n.3).
- “[O]n or about July 12, 2020, Austin communicated with the Thomas Cellphone using iMessage about meeting Thomas and Senior in Lower Manhattan. Two days later, on or about July 14, 2020, Austin sent the following iMessage to Thomas: “That shit Gone! I was gonna pull up on him to grab up some more but ima go to Atlanta today give me a cash app so I can send this bread I owe & tell him Ima need some more as soon as I touch back down.” Thomas then sent Austin a screenshot of a Cashapp Account with the screenname “\$casanovaa2x.” Based on my training, experience and involvement in this investigation, I believe Austin coordinated with Thomas to pick up a supply of narcotics from Senior—consistent with what Soto has told the CI [see next sentence]—and that Thomas then sent Austin a screenshot of Senior’s Cashapp account so that Austin could pay Senior directly.” “During [a] recorded buy of crack cocaine on July 30, 2020, [a] CI [confidential informant] told Soto, in substance and in part, that Casanova’s manager was his (Soto’s) supplier, and that Casanova supplied Austin.”<sup>3</sup> (*Id.* ¶¶ 36).
- “Based on my review of a subpoena return from Apple produced on August 21, 2020, I know that ... one of the cellphones listed on [Senior’s iCloud account] is the Senior Cellphone.” (*Id.* ¶ 28).
- Given the “storage and backup properties of Apple iCloud accounts” and Mr. Senior’s use of the Senior Cellphone to facilitate Gorilla Stone activity, “there is probable cause to believe that the information stored on [Mr. Senior’s iCloud] would constitute evidence of the Subject Offenses.” (*Id.* ¶¶ 13, 37, 39).<sup>4</sup>

The Magistrate issued a search warrant (the “iCloud Warrant”) based on the Agent’s affidavit, directing Apple to produce to the FBI, *inter alia*, the following:

---

<sup>2</sup> The Agent failed to explain why it only “appear[ed]” that some of these photos were published on an Instagram account used by Mr. Senior. The Agent did not use such ambiguous language with respect to photos allegedly posted to others’ Instagram accounts. (*See* Ex. A ¶¶ 28, 30 & n.2).

<sup>3</sup> Seemingly, the Agent meant that Soto made the statements to the CI. (*See* Aff. ¶ 36).

<sup>4</sup> The Agent did not allege or suggest that Mr. Senior ever set up his iCloud account, enabled it, and stored data on it.

- “[a]ll records or other information regarding the devices associated with, or used in connection with, [Mr. Senior’s iCloud]”; and
- “[t]he contents of all files and other records stored on iCloud,” including the “contents of all emails ... [and] instant messages associated with [Mr. Senior’s iCloud] from January 1, 2019 to August 24, 2020,”; “all iOS device backups”; “all ... app data”; “all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain”; “all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks”; and “[a]ll preserved records for the ... [a]ccount[.]”

(Ex. B, iCloud Warrant, Attach. A §§ I–II)). The iCloud Warrant then authorized law enforcement officers to review the records produced by Apple for “any evidence, fruits, and instrumentalities of [the Subject Offenses] between January 1, 2019 and August 24, 2020,” including “communications ... between Walter Luster, Deshawn Thomas, and Caswell Senior and co-conspirators regarding the Subject Offenses; “images showing evidence of the Subject Offenses”; and “[e]vidence of the underlying criminal enterprise discussed in the affidavit in support of this warrant, such as photographs of Luster, Thomas, Senior and co-conspirators together.” (*Id.*, Attach. A §§ I, III).<sup>5</sup> The iCloud Warrant did not provide any other details about the Subject Offenses. (*See generally* Ex. B).

The Government has produced to Mr. Senior almost 1.5 million records seized from his iCloud account, including thousands of “chat” files that originated from cellphones other than the Senior Cellphone. These materials include data of the most intimate nature, including photographs of Mr. Senior with his wife as well as communications between them and other personal matters entirely unrelated to this investigation.

---

<sup>5</sup> The iCloud Warrant functioned as “a hybrid of a traditional warrant and a subpoena.” *See United States v. Purcell*, 967 F.3d 159, 183 (2d Cir. 2020). The “‘search’ contemplated and authorized by the [warrant] was performed ... by [Apple], a private third party in possession of the potential evidence, and the ‘seizure’ was law enforcement’s receipt of material handed over by [Apple] under the terms specified by the warrant.” *See id.* at 181.

### III. The Operative Indictment

In the operative indictment, Mr. Senior is charged with RICO conspiracy; drug conspiracy; violent crimes (assault with a dangerous weapon and attempted murder) in aid of racketeering (“VICARs”); use of a firearm in furtherance of the drug conspiracy and the VICARs crimes; and gun trafficking. (ECF Doc. 245 (S6 Indict. ¶¶ 1–13, 41–44, 47–50, 55–58)).

### ARGUMENT

The iCloud Warrant violated the Fourth Amendment in numerous ways:

- a. The warrant authorized the wholesale seizure and review of Mr. Senior’s iCloud data even though there was no probable cause to believe that the iCloud account contained any evidence, let alone “extensive” evidence, of his suspected criminal activity. Although the agent swore that the Senior Cellphone was “listed” on his iCloud account, iCloud was built into the phone and there was no probable cause to believe that he had ever set up his iCloud account, enabled it, and backed up data on it. This, we respectfully submit, constitutes a fatal flaw in the granting of the warrant to search the entire iCloud account.
- b. There was no probable cause to believe that Mr. Senior had committed the Subject Offenses.
- c. Even if there was probable cause that Mr. Senior’s iCloud account contained stored data and that he committed some or all of the Subject Offenses, allegations that Mr. Senior used his cellphone an unidentified number of times to facilitate crimes did not provide reason to believe that criminal activity “pervaded” his iCloud account. As such, the warrant was overbroad in its sweeping authorization to search potentially the entire universe of Mr. Senior’s life.
- d. The warrant did not comport with the particularity requirement as defined by Fourth Amendment. The warrant *itself* did not provide any details about Mr. Senior’s suspected criminal activity other than referencing the names of co-conspirators, “the underlying criminal enterprise,” and several criminal statutes he allegedly violated. These inadequate parameters did not provide the executing officers with enough information to discern what iCloud data would constitute evidence of the suspected crimes. Instead, the warrant permitted the Government to seize and review a repository of a Mr. Senior’s entire life and then rummage through it on an unconstitutional fishing expedition merely on the basis that he allegedly used an Apple device to facilitate crimes.
- e. The iCloud Warrant did not include a temporal limitation as to the records Apple was ordered to produce to the FBI.

- f. The Warrant did not limit the records to be reviewed to the records that came from the sole digital device that Mr. Senior allegedly used to facilitate the Subject Offenses.
- g. Finally, the Warrant failed to instruct the Government as to what to do with any seized records that did not constitute evidence of the Subject Offenses.

As such, all information obtained or derived from the general search of Mr. Senior's iCloud account should be suppressed. *See Utah v. Strieff*, 579 U.S. 232, 237 (2016).

## **I. THE iCloud WARRANT VIOLATED THE FOURTH AMENDMENT**

The Fourth Amendment to the Constitution provides the following:

The right of the people to be secure in their ... effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Amendment is designed to prevent "general, exploratory rummaging in a person's belongings and the attendant privacy violations." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013).

The digital age has presented courts with significant challenges when assessing the propriety of warrants authorizing a search of a human being's entire universe of conduct and experiences. The seizure of iCloud data "can give the government possession of a vast trove of personal information about the person to whom the data belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." *Purcell*, 967 F.3d at 183. Such information could reveal the most "intimate details regarding an individual's thoughts, beliefs, and lifestyle," such as political beliefs, sexual preferences, and medical information. *See United States v. Ganas*, 755 F.3d 125, 135 (2d Cir. 2014), *on reh'g en banc*, 824 F.3d 199 (2d Cir. 2016); *see also Riley v. California*, 573 U.S. 373, 395, 403 (2014). Therefore, the Fourth Amendment "assumes even greater importance" when digital property is to be searched. *Galpin*, 720 F.3d at

446. This heightened scrutiny of the warrant to search of all Mr. Senior's iCloud data reveals its many constitutional defects.

**A. The Agent's Affidavit Did Not Provide Probable Cause to Believe that Evidence of the Subject Offenses Would be Found on Mr. Senior's iCloud Account**

In deciding whether to issue a search warrant, a magistrate “must make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Raymond*, 780 F.3d 105, 113 (2d Cir. 2015). A reviewing court, in turn, must ensure that the magistrate “had a substantial basis for his [probable cause] determination.” *Id.*

The iCloud Warrant was not supported by probable cause in two distinct respects. First, and we submit determinatively, the warrant broadly authorized the seizure and review of *all of Mr. Senior's iCloud data*, even though the Magistrate had no substantial basis for finding that his iCloud account contained any stored data (incriminating or otherwise). The Agent alleged in his affidavit that an Apple user *could* store data on iCloud, which “is built into every Apple device” (<https://www.apple.com/icloud/>), but made no allegations suggesting that Mr. Senior *ever actually used* the iCloud service. The Agent's allegations did not assert that Mr. Senior ever backed up the Senior Cellphone to his iCloud or otherwise stored data on it, let alone suggest that he ever enabled his iCloud or even set it up.<sup>6</sup> There was no allegation that the agent had divined from a subpoena or otherwise that there was anything stored on Mr. Senior's iCloud. The fact that others can and

---

<sup>6</sup> See <https://support.apple.com/guide/icloud/introduction-to-icloud-mm74e822f6de/icloud> (“To set up iCloud, you just sign in to your device with your Apple ID, then choose which apps you want to use with iCloud and which iCloud features you want to turn on or off.”); <https://support.apple.com/icloud> (“[Y]ou can choose what data to store in iCloud by turning features on or off.”); <https://support.apple.com/en-us/HT207689> (“When you turn [iCloud off for an app], the app will no longer connect with iCloud, so your data will exist only on your device. You can choose which apps on your device you'd like to use iCloud, or turn off iCloud completely.”).

do use a particular repository to store items did not, *a fortiori*, mean that Mr. Senior did.

An opinion by the Court of Appeals for the Armed Forces (“CAAF”) is instructive as it elucidates the insufficient nexus between the Senior Cellphone and his iCloud account. In *United States v. Nieto*, a military magistrate “issued a search and seizure authorization [i.e., a warrant] to search Appellant’s bunk and seize any cell phone or laptop computer that was found there.” 76 M.J. 101, 104 (C.A.A.F. 2017). The authorization was based on information that (a) Appellant used his cellphone to commit a crime, and (b) soldiers who take photos on their cellphones “normally ... back those [the photos] up to their laptops.” *Id.* at 103–04, 107. After agents of the Army Criminal Investigation Division (“CID”) seized a cellphone and laptop from Appellant, a different magistrate authorized the search of the two items. *Id.* at 104–05. This second authorization was based on an application by SA Dunn, who “relied on [CPL] RAO’s sworn statement, as well as on an affidavit that mirrored the previous affidavit, except for, *inter alia*, the following additional paragraph[]”:

It is my experience as a CID Special Agent that persons who would use a portable digital media recorder would also transfer the media from a portable device to a computer station or storage device. Persons who view and record sexual acts often times store and catalog their images and videos on larger storage devices such as a computer or hard drive.

*Id.*

A military judge denied Appellant’s motion to suppress the evidence seized from his laptop, and the United States Army Court of Criminal Appeals (“ACCA”) affirmed. *Id.* at 103, 105. The CAAF reversed the ACCA’s decision, concluding that there was an “insufficient particularized nexus linking Appellant’s misconduct to his laptop”:

[C]ell phones ... are in fact minicomputers that have immense storage capacity allowing them to store thousands of pictures, or hundreds of videos.... *Therefore, in this age of “smart phones,” SA Sandefur’s generalized profile about how*

*servicemembers “normally” store images was technologically outdated and was of little value in making a probable cause determination.*

We further note that the affidavits accompanying the search authorization did not reference a laptop or data transfers from Appellant’s cell phone. Accordingly, we conclude that SA Sandefur’s generalized profile was not based on a firm factual foundation. As a result, the information provided by SA Sandefur to the magistrate did not independently establish a particularized nexus between (a) the crime the accused was alleged to have committed with his cell phone in the latrine and (b) the laptop that was previously seen by ‘somebody’ on Appellant’s bunk.<sup>[7]</sup> In order to identify a substantial basis for concluding that probable cause existed to believe that Appellant’s laptop was linked to the crime, we conclude that—at a minimum—there needed to be some additional showing, such as the fact that Appellant *actually downloaded images (illicit or otherwise) from his cell phone to his laptop, stored images on his laptop, or transmitted images from his laptop.* And yet, there was no such showing in this case.

*Id.* at 103, 107–08 & n.3 (emphasis added). In reaching its conclusion, the CAAF was “mindful that a contrary holding could be construed as providing law enforcement with broad authority to search and seize *all* of an accused’s electronic devices and electronic media merely because the accused used a cell phone in furtherance of a crime.” *Id.* at 108 n.5. “This result, based on generalized profiles created by law enforcement and on the generalized observation about the ease with which digital media may be replicated on a multitude and array of electronic devices, would run counter to the principle that law enforcement officials must provide *specific and particular* information in order for a magistrate to determine that there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.*

Similarly, here, the fact that Mr. Senior had a cellphone that he *could* have used to store anything on his iCloud cannot, without more, suffice to establish probable cause to believe that he did so. In fact, unlike in *Nieto*, the Agent here provided no allegations suggesting that iPhone users

---

<sup>7</sup> In the course of SA Sandefur’s investigation, he “was told by his agents that ‘somebody’ had previously seen a ... laptop on Appellant’s bunk in his tent.” *Nieto*, 76 M.J. at 103; *see also id.* at 108 (“CID only knew that a laptop was on Appellant’s ‘bunk in his tent.’ When pressed on this specific point, SA Sandefur could not explain how CID learned of the laptop.”).

normally back up their cellphone data onto iCloud. This alone, we respectfully submit, is sufficient grounds to controvert the warrant and suppress any and all fruits derived from the search.

Second, there was no probable cause to believe that Mr. Senior committed the Subject Offenses. The Magistrate had no substantial basis for finding that Mr. Senior had committed the suspected firearm or VICAR crimes. In his affidavit, the Agent's only allegations as to Mr. Senior were that he was with Luster on the same day that *Luster* posted on Instagram a photo of *himself* holding a gun. There was no indication that Luster's Instagram photo was taken on (or even about) the same day it was published or that Mr. Senior was near Luster when the photo was taken. Even if Mr. Senior was near Luster when the photo was taken, that fact provides insufficient cause that Mr. Senior himself possessed a gun or aided Luster in his possession of a weapon. Indeed, there is no evidence that Luster was holding a real gun. A contrary finding would authorize search warrants against anyone who was with a person on the same day that the latter person published a photo of himself holding a gun, real or not.

Moreover, there were no allegations indicating that Mr. Senior possessed a weapon in furtherance of a drug trafficking or violent crime. None whatsoever. Nor were there any allegations that Mr. Senior committed any acts of violence. Accordingly, the iCloud Warrant should not have authorized the executing officers to seize or examine evidence of the suspected firearm or VICAR crimes.

With respect to narcotics trafficking, the Agent alleged that after Ms. Austin asked Mr. Thomas to "give [her] a cash app so [she] can send this bread [she] owe[d]," he sent her a screenshot of Mr. Senior's Cashapp account.<sup>8</sup> But there was no probable cause that Mr. Senior was

---

<sup>8</sup> Other than voice calls, Cashapp, and apparently some Instagram photos, the sources of the Agent's allegations about Senior committing crimes came from statements made by Soto, Austin, and Thomas; Instagram photos posted by Luster and Thomas; and contents from Gillard's iCloud account.

involved in the apparent drug transaction. Even if Mr. Thomas told Ms. Austin to send the proceeds of a drug sale to Mr. Senior's Cashapp account, there was no evidence that Mr. Senior actually sold her or anyone drugs. Mr. Senior could have been owed that money for a non-drug sale purpose. Thomas may have simply wanted the money sent to Senior for any number of reasons. Palpably absent from this affidavit are *any* messages to or from Senior suggesting his complicity in whatever Austin and Thomas were discussing.<sup>9</sup> Given the dearth of evidence relating to these substantive crimes, there was insufficient evidence to establish probable cause that Mr. Senior was involved in any racketeering.

Based upon the foregoing, the affidavit in support of the iCloud Warrant failed to establish probable cause.

#### **B. The iCloud Warrant was Fatally Overbroad**

Warrants that “authorize broad searches of both digital and non-digital locations may be constitutional, so long as probable cause supports the belief that the location to be searched—be it a drug dealer’s home, an office’s file cabinets, or an individual’s laptop—contains extensive evidence of suspected crimes.” *Purcell*, 967 F.3d at 181. “The doctrine of overbreadth represents, in a sense, an intersection point for probable cause and particularity principles: it recognizes, in pertinent part, that a warrant’s unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause.” *United States v. Wey*, 256 F. Supp. 3d 355, 382 (S.D.N.Y. 2017) (Nathan, J.); *see also In re 650 Fifth Ave. & Related Properties*, 830 F.3d 66, 99 (2d Cir. 2016).

---

<sup>9</sup> The Agent did not explain what, if any, records from a Cashapp transaction could get stored on iCloud. Moreover, the Agent did not mention even one single message to or from Mr. Senior despite the fact that the Government had access to the cellphone activities of Ms. Austin and other Codefendants. (*See, e.g., Ex. A, ¶ 36*).

“[W]arrants will frequently lack particularity where they include a general, catch-all paragraph or provision, often one authorizing the seizure of any or all records of a particular type.” *United States v. Drago*, No. 18-cr-394, 2019 WL 4364644, at \*8 (E.D.N.Y. June 25, 2019) (Shields, M.J.), *report and recommendation adopted*, 2019 WL 3072288 (E.D.N.Y. July 15, 2019) (Feuerstein, J.).

Even assuming, *arguendo*, the existence of probable cause to search Mr. Senior’s iCloud account, given the breadth of the search authorized—an entire iCloud account potentially spanning years—the relevant inquiry is whether there was probable cause to believe that the account was “pervaded” with evidence of the Subject Offenses such that compartmentalizing the search was simply unnecessary.

The “extensive evidence” rule is an extension based on the “all-records exception,” which provides that when “criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements.” *U.S. Postal Serv. v. C.E.C. Servs.*, 869 F.2d 184, 187 (2d Cir. 1989) (cited in *Purcell*, 967 F.3d at 179, 181). The “Fourth Amendment requires more than mere extrapolation to activate the all-records principle.” *Wey*, 256 F. Supp. 3d at 389. Although “the probable cause showing necessary to invoke the all-records exception is always substantial, the Government faces an even higher hurdle than usual in attempting to apply it to” a residence (as opposed to a business).” *Id.* “Indeed, as several Circuits have recognized, [issuance of an all records search of a residence] would require extraordinary proof to demonstrate that an individual’s entire life is consumed by fraud and that *all* records found in the home were subject to seizure.” *Id.*; see *United States v. Humphrey*, 104 F.3d 65, 69 & n.2 (5th Cir. 1997). This principle logically extends with greater force to an “all records” search of a person’s cloud storage repository.

Judge Kenneth M. Karas’s opinion in *United States v. Vilar*, No. 05-cr-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007), is instructive. In *Vilar*, a magistrate issued a warrant authorizing the government to search offices of Defendants’ corporation, Amerindo Investment Advisors Inc., and seize “documents relating to the three allegedly misused investment funds”; “the three suspicious accounts”; “the two groups of victims”; and “*all* client files, *all* investment advisory agreements, and *all* documents concerning communications with Amerindo clients, regardless of whether those documents had any relation to the funds, accounts, and individuals addressed by the Warrant application.” *Id.* at 1, 3, 7, 20. The Government tried “to justify the breadth of the search by claiming that Amerindo was permeated by fraud and therefore that the ‘all-records’ exception applie[d].” *Id.* at 4. Judge Karas rejected the argument, finding that “the warrant application fail[ed] to establish that the evidence presented in the application [wa]s just the tip of the iceberg or that Defendant’s operation was, solely and entirely, a scheme to defraud” *Id.* at 21.

Similarly, here, the Agent’s affidavit provided no probable cause that Mr. Senior’s iCloud account was “permeated” with the suspected criminal activity. Rather, the affidavit simply asked permission to search the entire account to look for some. Apple users are provided “with five gigabytes of free electronic space on iCloud,” but the Agent’s affidavit consisted only of (at most) a few alleged instances where Mr. Senior used his cellphone (voice calls, Cashapp, and apparently Instagram) to facilitate the suspected criminal activity. Thus even assuming that the Agent’s affidavit provided probable cause that Mr. Senior used his iCloud account, there were no allegations suggesting that the account was devoid of records pertaining to “legitimate ... activities” or even that they actually contained evidence of criminality. *See Vilar*, 2007 WL 1075041, at 21. Mr. Senior was a successful rap artist with a contract from Roc Nation and other legitimate business dealings. He was married with a child and was otherwise involved in lawful

endeavors. Even if there was probable cause to believe that Mr. Senior had set up his iCloud, enabled it, and stored data on it, there was still no probable cause that the iCloud account contained “extensive” evidence of the Subject Offenses to justify the wholesale search authorized. The isolated evidence cited by the Government was a far cry from establishing probable cause that the suspected criminal activity “pervaded” Mr. Senior’s “entire” iCloud account. *Cf. Purcell*, 967 F.3d at 181; *cf. id.* at 174–75, 181 (finding that “there was reason to believe that the suspected [prostitution] activity pervaded” the defendant’s “entire” Facebook account, and thus “seizure of all records of the account was appropriate,” where he made public Facebook posts (1) “in which [he] repeatedly referred to himself as a ‘pimp’ and discussed women (referred to as ‘bitches’) earning money for him and ‘selling themselves for’ him” and (2) “that suggested [that the account] was being used to recruit ‘numerous female individuals to come work in prostitution.’”).

Based upon the foregoing, the warrant was fatally overbroad.

### **C. The iCloud Warrant Was Insufficiently Particular**

The iCloud Warrant was also insufficiently particular. To satisfy the Fourth Amendment’s particularity requirement, a warrant must “identify the specific offense for which [the government] ha[s] established probable cause.” *Galpin*, 720 F.3d at 445–46. A court “may tolerate some ambiguity in the warrant so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.” *Id.* at 446. “[A] failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect’s privacy and property are no more than absolutely necessary.” *Id.*; *see also Kow*, 58 F.3d at 427 (“Generic classifications in a warrant are

acceptable only when a more precise description is not possible.”<sup>10</sup>

“[B]ecause there is currently no way to ascertain the content of a [digital] file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, by necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.” *Galpin*, 720 F.3d at 447. “Once the government has obtained authorization to search [a storage] drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant.” *Id.* “There is, thus, a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” *Id.* “This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.” *Id.*

Here, the *iCloud Warrant* failed to sufficiently describe Mr. Senior’s suspected criminal activities. Although the Agent’s *affidavit* provided more detail about Gorilla Stone and Mr. Senior’s suspected criminal activities, the “Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.” *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). The affidavit frames the issues for the magistrate. The warrant is the permissive instrument that must guide the search to protect the privacy interests embodied in the Fourth Amendment.

The iCloud Warrant’s only references to any potentially suspected crimes were the names of Luster and Thomas; “co-conspirators”; “the underlying criminal enterprise”; and the criminal statutes allegedly violated by Mr. Senior. The iCloud Warrant did not even mention the name

---

<sup>10</sup> The “particularity requirement serves three related purposes: preventing general searches, preventing the seizure of objects upon the mistaken assumption that they fall within the magistrate’s authorization, and preventing the issuance of warrants without a substantial factual basis.” *United States v. Young*, 745 F.2d 733, 759 (2d Cir. 1984).

Gorilla Stone, let alone suggest that the underlying investigation involved a gang. Thus, the Warrant authorized officers to review all of Mr. Senior's iCloud data for evidence of *any* RICO crime, drug trafficking conspiracy, gun possession crime, or "criminal enterprise"—even if those crimes or the "enterprise" were completely unrelated to Mr. Senior's alleged role in the Gorilla Stone or other suspected criminal activities. Because the iCloud Warrant "[m]ere[ly] referenced ... 'evidence' of a violation of ... broad criminal statute[s] or general criminal activity," the warrant "provide[d] no readily ascertainable guidelines for the executing officers as to what items to seize." *See United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992).<sup>11</sup>

Moreover, the iCloud Warrant was not as particular as the circumstances reasonably allowed. *See Galpin*, 720 F.3d at 446. The underlying criminal investigation began in or about March 2020, and the Agent spent over ten pages of his August 2020 affidavit describing the Gorilla Stone as well as acts allegedly committed by Mr. Senior and co-conspirators in furtherance of the

---

<sup>11</sup> *See also United States v. Whitten*, 706 F.2d 1000, 1014–15 (9th Cir. 1983) (finding that a warrant authorizing a search for "evidence of narcotics trafficking" was overbroad because it did "not enable the officers executing it to confine their search to particular items whose seizure was authorized by the issuing magistrate"), *overruled on other grounds, United States v. Perez*, 116 F.3d 840 (9th Cir. 1997); *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) ("'[L]imiting' the search to only records that are evidence of the violation of a certain statute is generally not enough.... If items that are illegal, fraudulent, or evidence of illegality are sought, the warrant must contain some guidelines to aid the determination of what may or may not be seized."); *United States v. Vilar*, No. 05-cr-621, 2007 WL 1075041, at \*22 (S.D.N.Y. Apr. 4, 2007) (Karas, J.) ("[N]owhere does the Warrant indicate what specific acts of wrongdoing are being investigated. Paragraph 16 of the Warrant Rider contains an oblique reference to 'participants in the fraud schemes,' but this would have been unhelpful to the Inspectors executing the search, as the Warrant does not identify those participants or explain the referenced fraud schemes, nor does it identify the particular transactions and illicit activities upon which the Warrant was founded."); *United States v. Gigante*, 979 F. Supp. 959, 966–67 (S.D.N.Y. 1997) (Rakoff, J.) ("[C]ategory '(5),' by authorizing searches and seizures of evidence relating to violations of such an immensely broad statute as 18 U.S.C. § 1962 ('RICO'), seemingly provides no limits at all. Furthermore, the sheer volume of documents seized in the execution of the warrants arguably evidences the possibility that the warrant did not enable the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." (citing, *inter alia*, *George*, 975 F.2d at 75–76)).

gang. However, the iCloud Warrant’s references to Mr. Senior’s suspected criminal activities were limited to Luster’s and Thomas’s names, unidentified “co-conspirators,” an unidentified “criminal enterprise,” and several enumerated criminal statutes. *See Kow*, 58 F.3d at 427 (finding warrant insufficiently particular where the Government failed to “contain the scope of the warrant by reference to limiting descriptions in the [supporting] affidavit”); *United States v. Roche*, 614 F.2d 6, 7–8 (1st Cir. 1980) (“[T]he government could have limited the objects of search and seizure to documents and records pertaining to automobile insurance, but declined to do so. This impermissibly broadened the scope of the search beyond the foundation of probable cause.”).

The Second Circuit’s *Galpin* opinion is instructive. In *Galpin*, a judge issued a warrant to search the defendant’s “residence, vehicle, and person for property ‘believed to contain evidence that will constitute, substantiate or support violations of NYS Corrections Law, section 168–f subdivision four, NYS Penal Law and or Federal Statutes.’”<sup>12</sup> 720 F.3d at 441. The warrant permitted the search of computers, central processing units, external and internal drives, storage units, and several other repositories of information. *Id.* at 441.

After finding that the warrant’s references to child porn images and “violations of ... NYS Penal Law and or Federal Statutes” rendered the warrant “facially overbroad,”<sup>13</sup> the Second Circuit concluded that “carv[ing] out the portions of the warrant authorizing a search for evidence of a registration offense from the constitutionality infirm remainder” would not have cured the warrant’s “apparent overbreadth”:

[T]he first and second paragraphs of the warrant would still broadly authorize a search of [the enumerated items] for any evidence substantiating a registration violation, without providing the forensic examiner [the one who

---

<sup>12</sup> N.Y. Correction Law § 168-f(4) requires sex offenders to register certain internet accounts and identifiers after a change of address. *Galpin*, 720 F.3d at 439 nn.1–2 (citing § 168-f(4)).

<sup>13</sup> The “warrant application failed to establish probable cause to search for evidence of child pornography,” and “the warrant’s references to the New York State Penal Law and ‘Federal Statutes’ were impermissibly broad.” *Galpin*, 720 F.3d at 447–48, 453.

reviewed the seized items] with any guidance or limitations as to what kinds of files might be relevant. While those provisions describe the places to be searched, they do not describe with adequate particularity the *items to be seized* by their relation to designated crimes. The third paragraph of the warrant particularizes the items that the government may seize, but nothing in the current record explains how the vast majority of those items—*e.g.*, access numbers, passwords, and PINS relating to voice mail systems, computing or data processing literature (including written materials), audio or video cassette tape recordings, books, and magazines—could possibly reveal evidence that Galpin possessed or used an unregistered internet account or communication identity.

*Id.* at 447–50 (2d Cir. 2013).

So too here, numerous clauses in the iCloud Warrant were insufficiently linked to the Subject Offenses. The iCloud Warrant authorized a review of all of Mr. Senior’s iCloud data for any evidence substantiating violations of several enumerated criminal statutes, without providing the executing officers “with any guidance or limitations [except a temporal limitation] as to what kinds of files might be relevant.” Similarly, the record is far from clear how any and *all* records that may have been stored in Mr. Senior’s iCloud could have “possibly reveal[ed] evidence” that he engaged in racketeering activities, conspired to distribute dugs, or possessed a gun.

#### **D. Other Unconstitutional Infirmities of the iCloud Warrant**

In addition to being overbroad and insufficiently particular for the above-mentioned reasons, the iCloud Warrant violated the Fourth Amendment in numerous other ways.

##### *Lack of Temporal Limitations*

The Warrant included no temporal limitation to the records Apple was required to produce to the Government, and thus allowed the Government to seize and review records dating back arbitrarily far. iCloud accounts store information indefinitely, as long as the user has sufficient storage. To plead a temporal scope of 18 months and then seek access to a lifetime of information is clearly an unauthorized intrusion into a person’s constitutionally protected privacy interests. *See Kow*, 58 F.3d at 427 (finding a warrant to be insufficiently particular, in part because the

“government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place, even though [the supporting] affidavit indicates that the alleged criminal activity began relatively late in [the defendants’ business’s] existence”); *Wey*, 256 F. Supp. 3d at 381; *United States v. Shipp*, 392 F. Supp. 3d 300, 310–11 (E.D.N.Y. 2019) (Garaufis, J.)

#### *Authorization to Search All Devices*

The iCloud Warrant impermissibly authorized the seizure and review of information that came from devices other than the Senior Cellphone, the sole device that he allegedly used to facilitate crimes. Although numerous devices could have been associated with Mr. Senior’s iCloud account (such as iPads or computers), the iCloud Warrant failed to limit the search and seizure to data that came from the Senior Cellphone. *See United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (“[The warrant] broadly authorized seizure of *all* cell phones and electronic devices, without regard to ownership. That expansive sweep far outstripped the police’s proffered justification for entering the home—viz., to recover any devices owned by Griffith.”). The iCloud Warrant in this case explicitly authorized the Government to seize and review all “information regarding the devices associated with, or used in connection with, [Mr. Senior’s iCloud].” The Agent himself acknowledged that a cellphone other than the Senior Cellphone was associated with his iCloud. (Ex. A ¶ 29 (Agent stating that the Senior Cellphone is “one of the cellphones listed on” his iCloud)).

#### *Evidence Unrelated to the Subject Offenses*

Third, and finally, the iCloud Warrant “did not set any limits on what the Government was required to do with the information that they” seized and reviewed, but did not constitute evidence of the Subject Offenses. *See Shipp*, 392 F. Supp. 3d at 311. “This is concerning in light of the

breadth of information that [Apple] was required to provide to the Government pursuant to the [iCloud] Warrant.” *See id.*

**II. THE GOVERNMENT SHOULD BE REQUIRED TO PROVIDE 404(B) EVIDENCE SIXTY DAYS BEFORE TRIAL**

This request is made pursuant to Fed. R. Crim. P. 16(a)(1)(c) and, as such, we ask that the Government be directed to disclose any and all acts that the Government intends to introduce pursuant to Rule 404(b) in such time so as to permit sufficient time for the defense to move to preclude the introduction of such evidence. We ask that this notice be provided well in advance of trial as it is likely that some such acts will date back several months or years and in order for the defense to effectively investigate and posit cogent and meritorious arguments in support of preclusion, sufficient notice is required. Additionally, in some circumstances the evidence sought to be admitted would warrant consideration of severance of defendants should the Government move to join any indictments. We respectfully submit that this evidence is discoverable pursuant to Rule 16 as it is “material to the preparation of the defense,” and much of it constitutes evidence that the Government will introduce in its case-in-chief.

**III. THE GOVERNMENT SHOULD DISCLOSE ALL EXCULPATORY AND IMPEACHMENT MATERIAL FORTHWITH**

A prosecutor has a constitutional duty to disclose material, exculpatory evidence to the defense, regardless of whether defense counsel makes a specific request. *United States v. Bagley*, 473 U.S. 667, 682 (1985); *Brady v. Maryland*, 373 U.S. 83, 87 (1963). The duty extends not only to information relevant to guilt, but also to evidence that would tend to impeach the prosecution’s witnesses. *Bagley*, 473 U.S. at 676-77 (“When the reliability of a given witness may well be determinative of guilt or innocence, non-disclosure of evidence affecting credibility falls within the general rule of *Brady*.”); *Giglio v. United States*, 405 U.S. 150, 154 (1972).

Impeachment evidence has been deemed to fall within the standard of materiality for *Brady* purposes. *United States v. Wong*, 78 F.3d 73, 79 (2d Cir. 1996) (“Evidence of impeachment is material . . . where the likely impact on the witness’s credibility would have undermined a critical element of the prosecution’s case.”). Even if the prosecutor is not directly aware of the evidence sought herein, a *Brady/Giglio* violation can still occur if the evidence was in the prosecutor’s constructive possession. For example, in *Kyles v. Whitley*, 514 U.S. 419 (1995), the Supreme Court held that state prosecutors have a duty to disclose impeachment evidence known to the police, even if the prosecutors themselves were not actually aware of the information. Many of the crimes alleged in this case occurred in other states and were handled by state prosecutors. It is incumbent upon the prosecution in this case to make inquiries as to the existence of *Brady/Giglio* material from these jurisdictions and provide same to the defense. *See United States v. Agurs*, 427 U.S. 97, 108 (1976).

While the Government is not dutybound to provide us with a witness list at this time, any witnesses who have provided *Brady/Giglio* material to the Government must be disclosed. The defense moves, pursuant to *Kyles* and its progeny, for the production of (1) any contradictory or inconsistent statements made to any law enforcement personnel/prosecutors by any individual(s), regardless of whether the Government intends to call those individuals in its direct case; (2) any evidence that would tend to inculcate someone other than Mr. Senior in any count in the Indictment and/or overt act; and (3) or any evidence which is inconsistent with the theory of the Government's case, as set forth in its Indictment, as it pertains to the specific role or activities of Mr. Senior. The defendant requests the production of these statements or evidence, irrespective of whether the Government intends to call the individual cooperator(s) or potential codefendant(s) as a witness.

**RESERVATION CLAUSE**

Defendants respectfully reserve the right to file additional pretrial motions as the need arises, including motions to preclude the Government from introducing evidence obtained or derived from the wiretaps and motions to sever the Defendants' trials depending upon how many defendants remain and the evidence sought for admission against remaining co-defendants.

**CONCLUSION**

For the foregoing reasons, the Court should grant this joint motion in its entirety, suppress all information obtained or derived from the general seizure and review of Mr. Senior's iCloud data, and grant the other relief requested herein.

Dated: New York, NY  
March 22, 2022

Respectfully submitted

/s/ James Kousouros

James Kousouros, Esq.

Stuart Gold, Esq.

The Law Offices of James Kousouros

260 Madison Avenue, 22nd Floor

New York, NY 10016

P: (212) 532-1934

F: (212) 532-1939

james@kousouroslaw.com

stuart@kousouroslaw.com

*Counsel for Defendant Caswell Senior*